IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of Ellingson

Application No.: 09/585,678

Filed: June 1, 2000

For: CAPTURING AND ENCODING UNIQUE USER ATTRIBUTES IN MEDIA SIGNALS

Examiner: S. Patel

Date: October 3, 2005

Response Under 37 CFR § 1.116
Expedited Procedure

Art Unit 2621 Confirmation No. 4533

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on October 3, 2005, as First Class Mail in an envelope addressed to: MAIL STOP AF, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450.

William Y. Conwell
Attorney for Applicant

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MAIL STOP AF
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant requests review of the final rejection in the above-identified application. No amendment is being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheets. (No more than 5 pages are provided.)

Date: October 3, 2005

Respectfully submitted,
DIGIMARC CORPORATION

By_____
William Y. Conwell
Registration No. 31,943
Attorney of Record

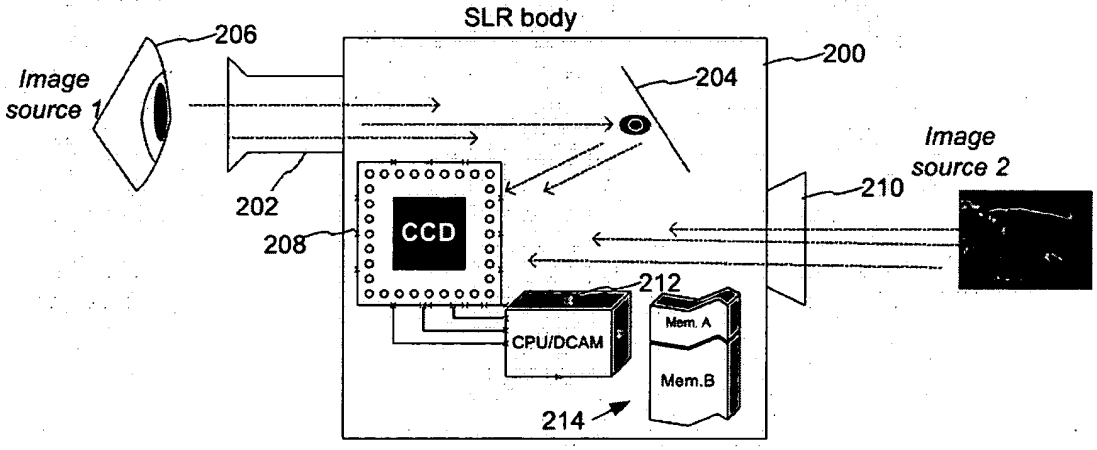
Customer Number 23735

Telephone: 503-469-4800
FAX: 503-469-4777

REASONS FOR PRE-APPEAL BRIEF REQUEST FOR REVIEW

One embodiment of applicant's invention is an SLR camera having a CCD that serves to image both (a) a subject (such as a landscape scene), and (b) attribute information about the operator of the camera (e.g., an image of the operator's eye (206)).

This embodiment is shown in Fig. 2 of the present application – excerpted below:



The first independent claim (29) encompasses this and other embodiments. It defines a method in which two types of information are captured:

1. Attribute information captured *from an operator*; and
2. Subject information captured *from a subject distinct from the operator*, under the control of the operator.

The method of claim 29 then requires that data related to (1) be encoded in data related to (2). (As further defined in the dependent claims, this encoding may be essentially imperceptible, e.g., by using steganographic techniques.)

The Final Rejection asserts that such an arrangement is taught by the principal reference, Borza (5,995,630). Applicant respectfully submits that the Office's reading of Borza is incorrect.

Borza teaches a biometric identification system. His detailed embodiment comprises a video system that has two modes of operation.

In the first mode, the fingerprint of the system operator is sensed by the system's CCD camera (using a prism optical arrangement shown in Borza's Fig. 8 and described at col. 11, lines 34-40). This fingerprint image is matched against a collection of previously-stored fingerprint data to identify the user.

In this first mode, once the captured fingerprint image is matched to determine the user's identity, the system looks up a particular cryptographic key corresponding to that user – a key which can then be used to encrypt and decrypt files associated with that user.

To help evade detection by third parties, this key is presented to the user *hidden in the fingerprint image sensed from the user.* Borza describes the advantages of this arrangement at col. 6, lines 48-66. (Illustrative data hiding arrangements are particularly detailed in Figs. 3d and 3e, and may involve substituting the least significant bits of certain image pixels with bits of the encryption key.)

In the second mode of Borza's system, biometrics are not involved. Borza's CCD serves simply as an imager for a video conferencing system. This is explained at col. 10, lines 50-57. (An image captured by the CCD is analyzed for the presence of biometric information – such as a fingerprint image. If none is sensed, the system simply serves as a plain video system – *no biometric operation or encoding is performed.*)

One of the Office's errors is in blurring these two modes of operation.

The second mode may meet the requirement of clause (b) of claim 29, *i.e.*, by capturing a video conference scene under the control of the operator. But in that second mode, the requirement of clause (a) is not met – no attribute information is captured *from the operator.*

The first mode may meet the requirement of clause (a), *i.e.*, by capturing a fingerprint image from an operator. But the requirement of clause (b) is then not met – there is no capture of subject information from a subject distinct from said operator, under control of the operator. (A fingerprint is not "a subject distinct from said operator.")

The language of clause (c) of claim 29 has antecedents in both clauses (a) and (b), so clause (c) is not met in either mode.

In Borza, the only teaching of an image captured under control of the operator, and into which data is encoded, is the captured fingerprint image. See, e.g., Borza's Fig. 3, below.

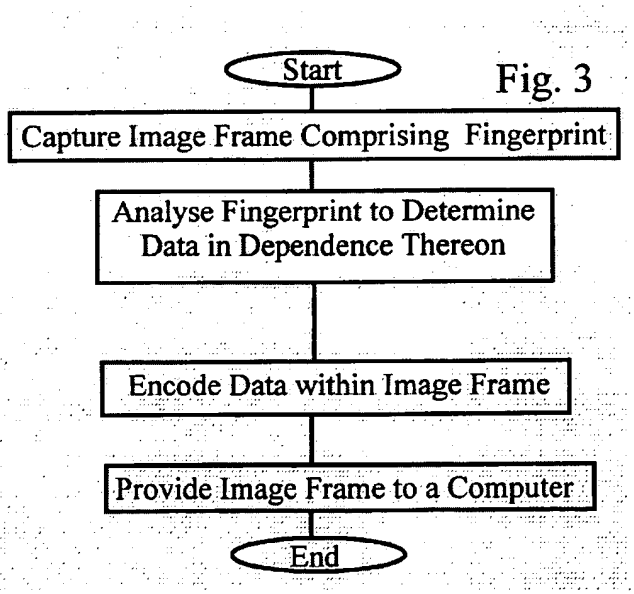


Fig. 3

The first rectangle is "Capture Image Frame Comprising Fingerprint." The third rectangle is "Encode Data within Image Frame." The only "Image Frame" contemplated in this mode of operation (*i.e.*, the Image Frame in which data is encoded) is the "Image Frame *Comprising Fingerprint*."

Put another way, Borza does not teach encoding of any data within imagery captured under control of the operator - *other* than within the fingerprint image captured

from the operator. Since such a fingerprint image is not "a subject distinct from said operator," as required by clause (b) of claim 29, the method is not anticipated.

The Examiner suggests that Borza can encode information in imagery other than the captured fingerprint image. There are some references in the specification to encoding of the cryptographic key within "*an* image frame," e.g., col. 6, lines 50-51. But read within the context of the document, it is evident that the image frame to which Borza refers is the frame of fingerprint data.

In the first sentence of the fourth paragraph under *Response to Arguments* found on page 2 of the Final Rejection, the Office cites col. 10, lines 50-56 (which teaches capture of subject information from a subject distinct from the operator) and also cites col. 7, lines 3-6 (which teaches capture of the user fingerprint). However, these two excerpts are drawn from *different* sections of Borza's specification, describing his two *different* modes of operation. The former is drawn from his second mode of operation - the one that has nothing to do with biometrics (in which his CCD serves as a plain video conferencing camera). No encoding is involved in this mode of operation.

Thus, Borza does not teach an arrangement in which data related to attribute information captured from the operator (such as a key associatively-related to a particular operator's fingerprint) is encoded in data related to a subject captured from a subject *distinct* from the operator, under control of the operator – all as required by claim 29.

This error in the Office's reading of Borza taints all of the rejections in the Final Action (each of which is premised entirely, or principally, on Borza). Accordingly, applicant does not belabor this paper by addressing other points concerning the claims, the rejections, and the cited art.

Favorable reconsideration is solicited.

Respectfully submitted,
DIGIMARC CORPORATION

Date: October 3, 2005

By _____
William Y. Conwell
Registration No. 31,943
Attorney of Record

Customer Number 23735

Telephone: 503-469-4800
FAX: 503-469-4777